VULNERABILITY AND PENETRATION TESTING

RECONAISSANCE
Obtain info on OS, network and IP

BLACK BOX
No knowledge of the system.Requires high level hacker skills and experience

Scope
What kind of access to system is at hand

GREY BOX
Partial knowledge of network

WHITE BOX
Full knowledge of system, 100 % overview of vulnerabilies

STATIC
Analyse system code. No hacks or exploits are processed.
pros: No potential damage to system
cons: Time consuming

MANUAL
Experienced hacker tries known strategies to discover vulnerabilities.
pros: Cheap and Fast
cons: Exploitation, need to recover

ASSESSMENT
Find potential vulnerabilities

STRATEGY
Asses list of vulnerabilites and plan best strategy to penetrate and exploit system

AUTOMATION
Robotic testing tools. Perform multiple methods quickly.
pros: Accuracy, Speed, multiple use
cons: Expensive, can't adapt

TOP TOOLS

METASPLOIT
NESSUS
KALI LINUX
BURP SUITE
W3AF
OPENVAS
PAROS PROXY
NEXPOSE
GFI LANGUARD
ACUNETIX WVS
QUALYSGUARD
MBSA
APPSCAN
CANVAS

NOISE
Inject random code which will make system crash. Then asses problems.
pros: expose vulnerabilities in event of crash, less human imntercation

HACK
Penetrate system. Once in enhance privelages to max

EXPLOIT
Explore and execute the potential hack

RESULTS
Acquire results and full outcome of hack

DOCUMENTATION
Document full outcome and results of VAPT and recommend solution for mana gemanent to asses the actions needed to restore security

RECOVER
Restore system and apply neccesary actions

OUTCOME
System is now a step ahead of any potential hack, elimiting any vulnerabilities and security risks that could otherwise be exploited by a real heacker